Microsoft

Operating System

Administering Certificate Services

Beta 3 Technical Walkthrough

Abstract

The administration model for Certificate Services in the Microsoft® Windows® 2000 operating system is based on using a Microsoft Management Console (MMC) snap-in. Those who are familiar with the previous release of the Microsoft Certificate Server (version 1.0) will recognize that this is a change from the Web-based model used in that prior release.

Using an MMC snap-in provides a highly scalable and extensible environment for Certificate Services administration. This technical walkthrough describes a number of useful tasks that can be performed with this new tool. In general, these tasks fall into the following categories:

- Service Administration—managing the server that issues certificates.
- Certificate Administration—managing the issued certificates.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0499

CONTENTS

INTRODUCTION

The administration model for Certificate Services in the Microsoft® Windows® 2000 operating system is based on using a Microsoft Management Console (MMC) snap-in. Those who are familiar with the previous release of the Microsoft Certificate Server (version 1.0) will recognize that this is a change from the Web-based model used in that prior release.

Using an MMC snap-in provides a highly scalable and extensible environment for Certificate Services administration. This technical walkthrough describes a number of useful tasks that can be performed with this new tool. In general, these tasks fall into the following categories:

- Service Administration—managing the server that issues certificates.
- Certificate Administration—managing the issued certificates.

The tasks described in this document are grouped into these categories.

As a prerequisite and as supporting information, you should be familiar with or have available the Certificate Services online documents provided with the Windows 2000 Server help files. The examples presented are based on the Stand-alone Certification Authority. See the Certificate Services online documents for a discussion of the Stand-alone and Enterprise Certification Authorities.

Be sure to review the section titled “Known Errors” prior to performing any of the tasks described here.

Prerequisites

To successfully complete this walkthrough, you should perform the following installations or walkthroughs and have obtained the following components.

- Install Windows 2000 Server at the Beta 3 RC0 level (Build 1946) or later
- Install a Stand-alone Certification Authority as described in the walkthrough titled “Setting up an Windows 2000 Certification Authority.”
- Populate the Certificate Services database with issued certificates sufficient to illustrate the principles (about 20 certificates should be sufficient). This should be done by repeating invocations of the enrollment scenario. See the walkthrough titled “Web Based Certificate Enrollment” for a description of how to obtain a certificate through enrollment.

  Note To create the sample data used in this walkthrough, you should create at least three certificates that contain the value *Finance* in the Organization field. Also note that using Web Enrollment makes the installation of Microsoft Internet Information Server a prerequisite. In this case, be sure that installation of Internet Information Server is completed prior to beginning the installation of Certificate Services. A second option for creating sample data is to use the **certreq** command-line utility. See the Certificate Services documentation for information on how to use this utility.

- Obtain another policy module. such as the Microsoft Visual Basic® programming system policy module (policyvb.dll) contained within the Platform SDK.

The first three itemsare required to begin the walkthrough. The last item is only required to perform the exercise in replacing the Certificate Services policy module.

SERVICE ADMINISTRATION

There are a number of tasks that an administrator performs as part of normal service operation. These include the following.

- Starting and stopping the service
- Backing up and restoring the service
- Configuring the policy and exit modules for use by the service

Each of these is described below.

In general, you need to have the following capabilities prior to administering a certificate services system.

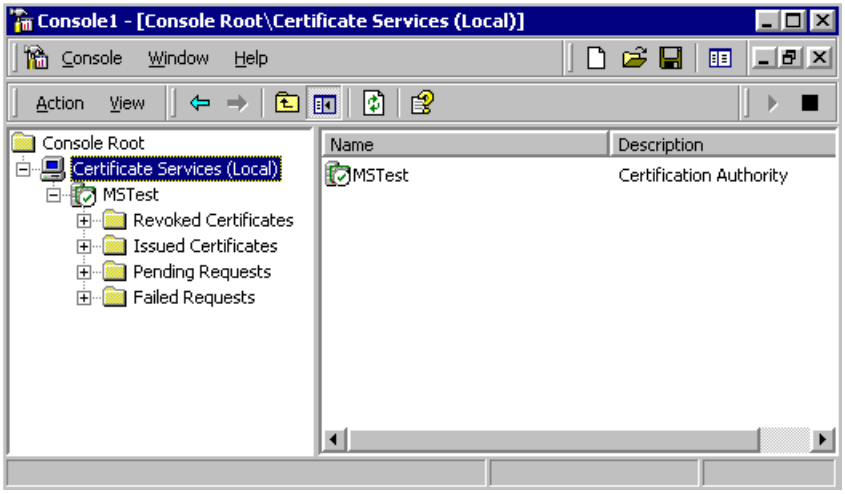
- Be logged on as a member of the Administrators or Certificate Server Administrators group that controls the certificate services system to be administered.
- Know the name of the certificate services system that you want to administer. This name is uniquely identified by the machine name and the Common Name (CN) of the Distinguished Name (DN) of the certification authority.
- Have added the Certificate Services Manager snap-in for the machine on which the certificate services system in question is running.

Start and Stop the Service

See the section on Known Errors at the end of this document prior to attempting this walkthrough.

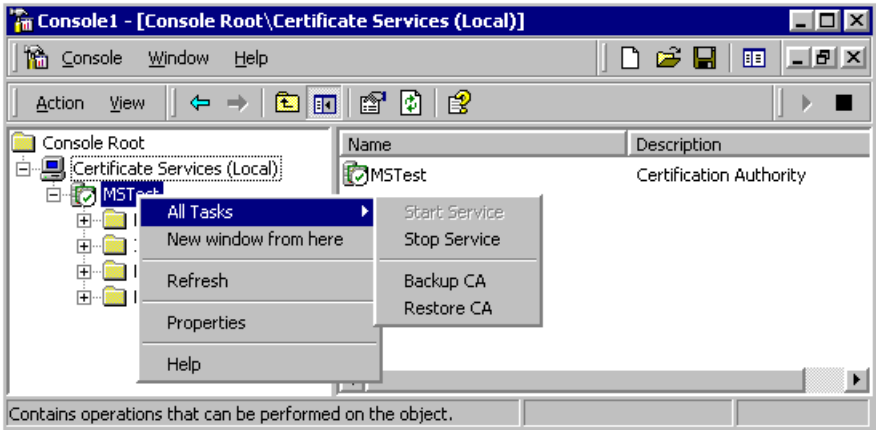
Starting Certificate Services is required to enable the receipt of certificate requests and the issuance of certificates. The service is automatically started following Certificate Services installation and on system reboot. Administrators may need to be able to manually stop or start the service as one mechanism to control the receipt of requests or issuance of certificates.

The following shows the basic MMC format. The sample Certification Authority (CA) is called *MSTest.*



To start and stop the Certificate Service

1. Right click the node with the**Common Name** (CN) of the certification authority in question (in this case, MSTest).
2. On the **Task** menu, select either the**Start Service** or **Stop Service** option, depending on what you are trying to do and the current state of the service.



Note In this image, the **Start Service** is grayed. This is because the service is currently operating, so starting it again is not a valid option. If the state of the service were reversed, the grayed item would be **Stop Service**.

Also, note that you can similarly stop or start the service by using the CD player buttons near the upper right corner; these buttons are grayed or highlighted based on the current state of the service.

Consider the case pictured above. In this case, the service is currently running. The **Start Service** option is grayed and the**Stop Service** option is highlighted. Stop the service by selecting the**Stop Service** option from the menu. You can tell that the service has been stopped by the fact that if you redisplay the menu, then the**Stop Service** menu item is grayed and the**Start Service** menu is highlighted. The CD

player buttons change in a similar manner—the **Stop** button is grayed and the **Start** button highlighted.

Note While the service is being stopped (or started), a progress menu and bar may be displayed.

Back Up and Restore the Service

See the section on Known Errors at the end of this document prior to attempting this walkthrough. Note that there is a known problem with restore in RC0. A workaround is described in the Known Errors section.

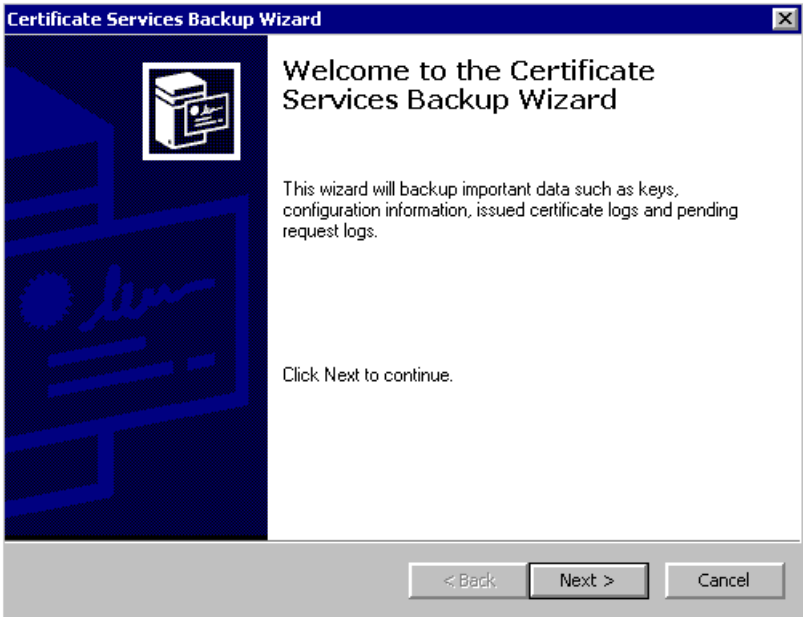
Certificate Services also provides a backup/restore tool that can perform selective backup of keys, certificates, and database (that is, the log of issued certificates and the queue of pending requests).

Administrators use this capability as part of their strategy for protection against catastrophic system or machine failures. Developing a recovery procedure that provides for periodic backups is highly recommended. This section describes backup and restore features available to administrators for this purpose.

Failure to implement such procedures means that you may be unable to preserve your audit trail of certificate requests and issued certificates, and you may lose the ability to revoke issued and previously unrevoked certificates.

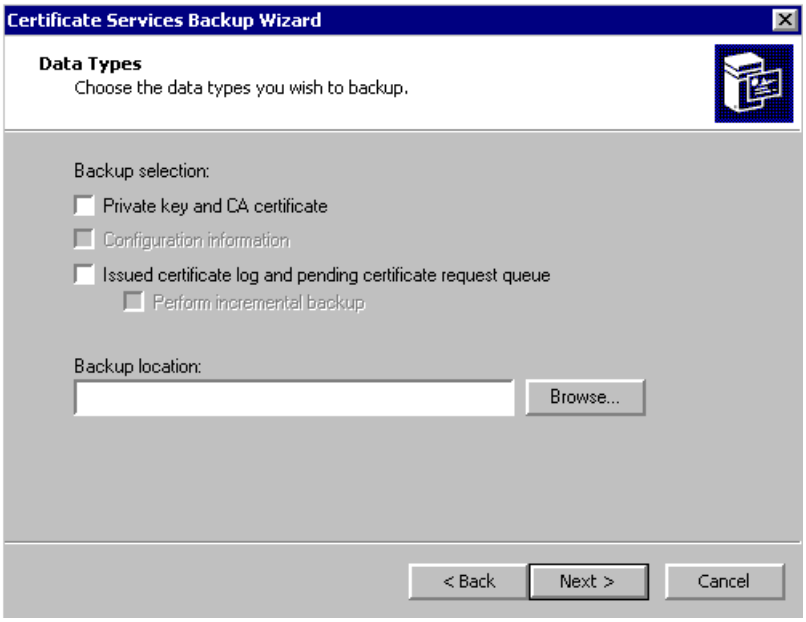
To back up and restore the Certificate Service

1. Select **Backup CA** to start the Backup/Restore wizard (as shown in the previous image). Click **Next**.

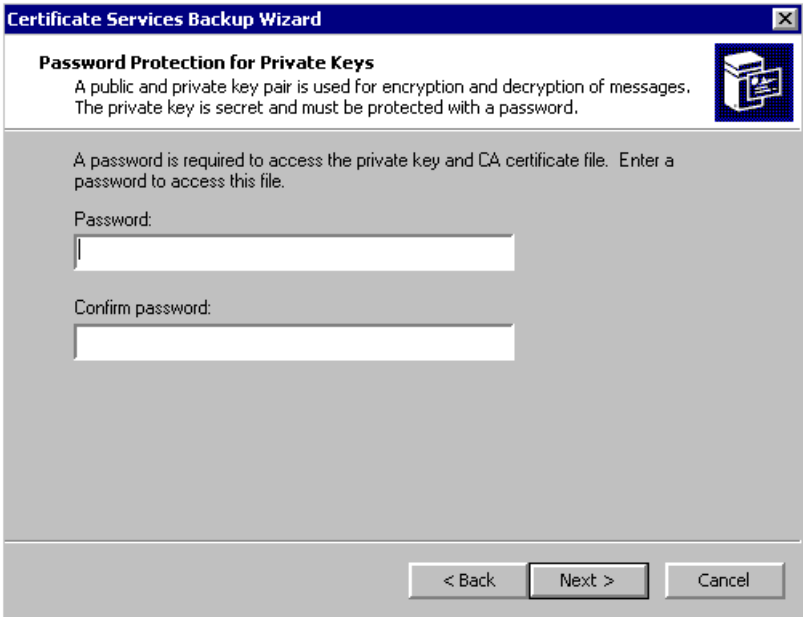


2. Check the boxes for the items to be included in the backup. (In this case, you will back up both the **Key/Certificate** and **log/queue**.) Check the box named "Private key and CA certificate." Check the box named "Issued certificate log and pending certificate request queue." Specify a folder for the backup in the input box by typing the name or select **Browse**. Click **Next**.

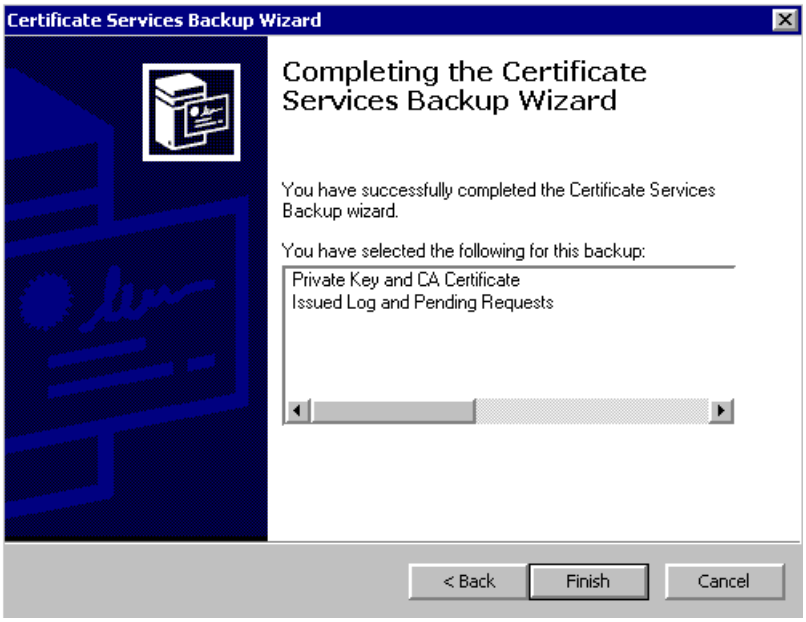
   Note The backup folder must be a preexisting folder.



3. Enter a **password** to be used to protect against subsequent access to the backup file by unauthorized persons. (Remember, the backup file includes the private key of the CA.) Click **Next**.



4. Both **Key/Certificate** and **Log/Queue** are displayed as backup options. Click **Finish**. The backup is now complete. A progress bar may be displayed while this is occurring.



The above form ceases to be displayed when backup is completed. This confirms backup. Secondary confirmation can be obtained by using either Windows Explorer or a command box to navigate to the location you supplied in step 2 above. In that folder, you should find a file with a *p12* suffix and a folder named DataBase. In the DataBase folder, you should find four files, one each with suffixes *.dat*, *.log*, *.pat*, and *.edb*. Secondarily, you can view the Application Event Log. There you will see numerous entries for Certificate Services (CertSvc) and the Data Base Engine (ESENT) that chronicle the backup activities. Specifically, look for the entries from the Data Base Engine that indicate that the backup activity was started and stopped.

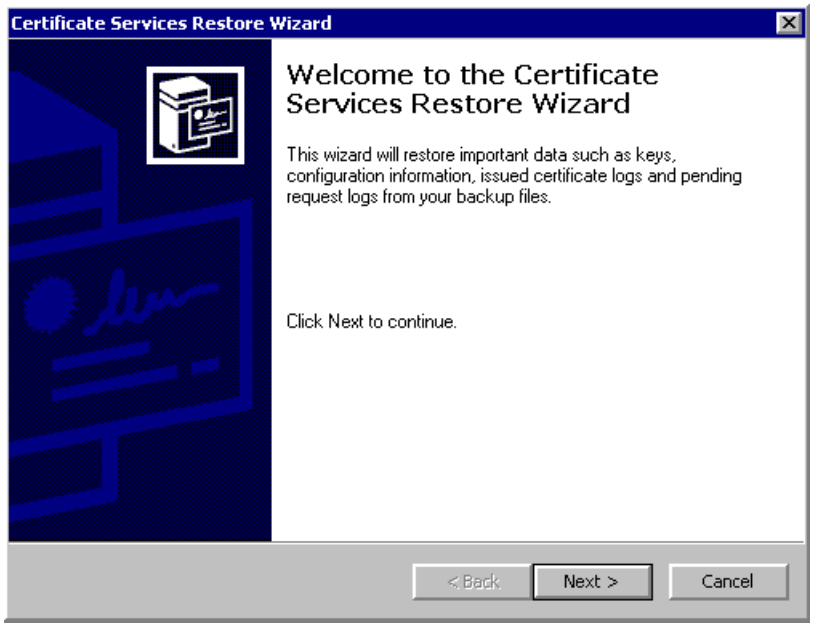
To restore the service from the backup:

See the section on Known Errors at the end of this document prior to attempting this walkthrough. Note that there is a known problem with restore in RC0. A workaround is described in the Known Errors section.

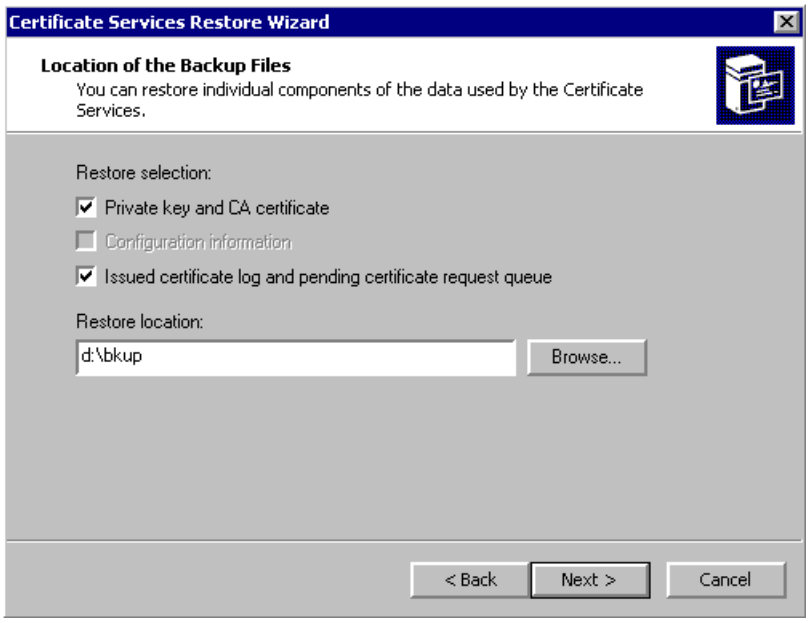
1. Start by right clicking the **Common Name of the certification authority** (in this example, **MSTest**). Select **Task** and **Restore CA**.
2. This starts the Certificate Services Restore wizard. If the Certificate Service is currently running, the following message is displayed.

3. Click **OK** to stop the service while the restore is in process.

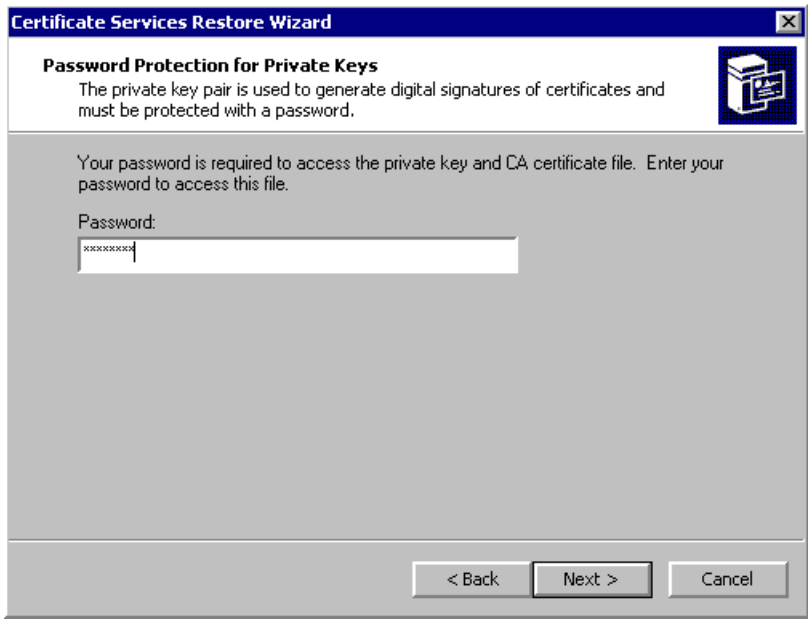
4. The service is stopped. A progress bar may display while this is happening. Afterwards, the wizard screen below appears. Click **Next**.



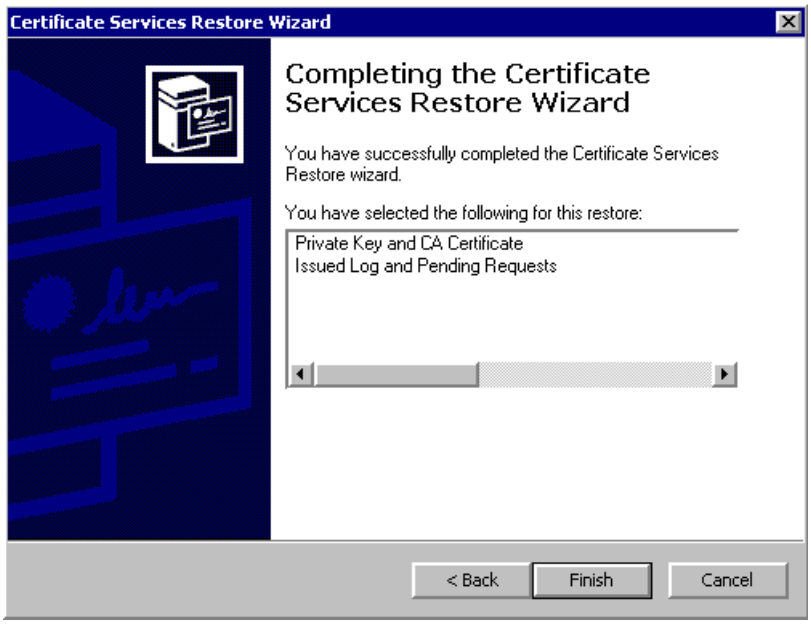
5. Check the appropriate boxes for what is to be restored (if you followed the instructions for backup as listed above, you should check the box titled “Private key and CA Certificate,” and the box titled “Issued certificate log and pending certificate request queue”), and enter the name of the backup folder in the input box. In this example, we’ve chosen to restore exactly what we backed up. Click **Next**.



6. Enter the password from the backup. Click**Next**.



7. Click **Finish**.



8. Once the restore is complete, the service restarts automatically. A progress bar is displayed duringrestart. Successful restart is your confirmation that restore is completed. Secondarily, you can look at the Application Event Log. Look for a message from the Data Base Engine (ESENT) that recovery steps have been completed.

Configure the Policy and Exit Modules for Use by the Service

See the section on Known Errors at the end of this document prior to attempting this walkthrough.

The Certificate Services architecture provides for replaceable policy and exit modules and processing. Policy modules incorporate decision logic that determines whether a certificate request should be approved, denied, or queued (left pending) for a later decision. Exit modules provide an opportunity to perform post-processing, such as publication of an issued certificate.

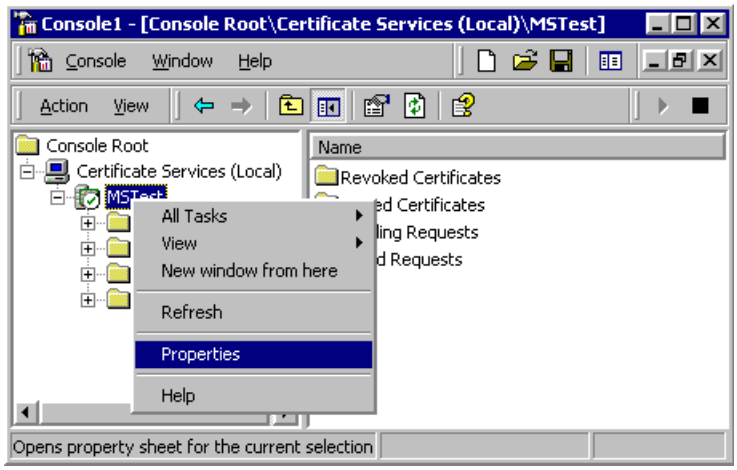
In this release, Certificate Services comes with a single policy module that incorporates two policies (Enterprise and default Stand Alone – see the Certificate Services documentation for an explanation of the differences) and one exit module (Enterprise). Starting with this release, users can replace these with their own modules. This is important for users that want to implement their own policy modules using the Platform SDK or who acquire third-party policy modules.

This walkthrough demonstrates how this works by providing an example of replacing the default policy module with a sample user-written module. Exit module management is performed in an analogous manner, but is not demonstrated here.

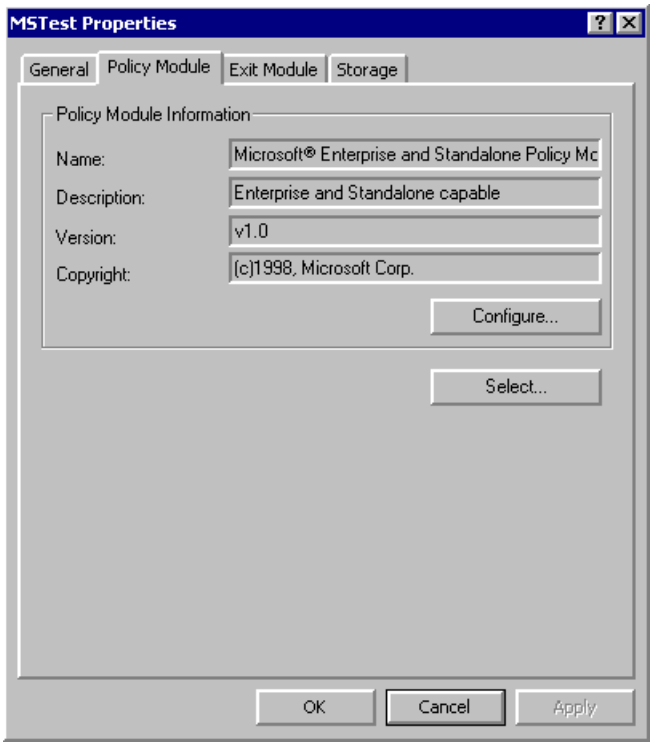
Note To perform this walkthrough, you need access to a second policy module, such as the Visual Basic sample policy module (policyvb.dll) available with the Platform SDK.

To configure the policy and exit modules for use by the service

1. Copy the **new policy module** to **%windir%\system32**.
2. Register the new policy module using the regsvr32 command.
3. From the **Certificate Services snap-in**, right click the **Common Name** (CN) of the certification authority in question (in this case, MSTest) and select **Properties**.

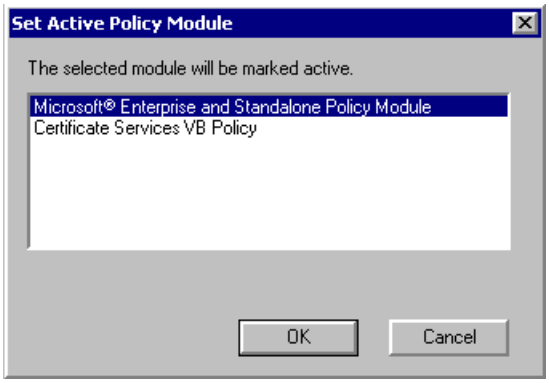


4. Select the **Policy Module** tab.

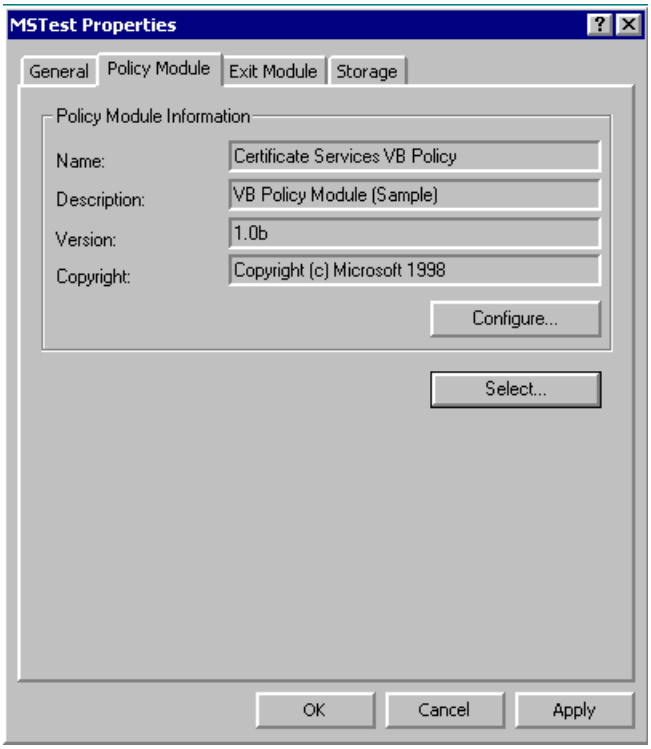


5. Click **Select**.

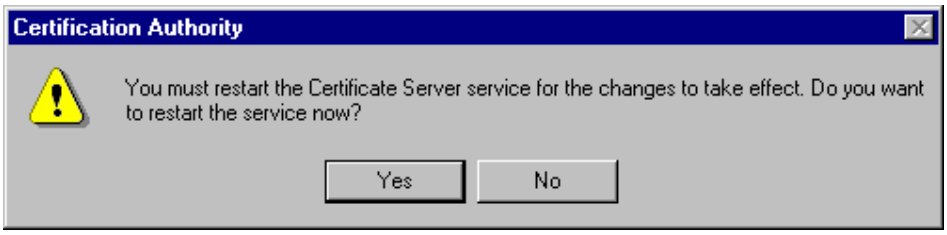
Select the new policy module to be installed (in this example, **Certificate Services VB Policy**). Click **OK**.



6. Click **Apply**.



7. Click **Yes** and then click **OK**. A progress bar is displayed as the service is stopped and restarted.



To verify that policy module replacement has been successful, look in the Application Event Log for records showing that the service (CertSvc) and Data Base Engine (ESENT) have been stopped and started. Also look at the property page and **Policy** tab (as described previously). The named policy module should be the new policy module.

CERTIFICATE ADMINISTRATION

This section describes common tasks an administrator must perform to manage the certificates issued by a Certificate Services system. These include:

- Displaying the Certificate Services Log and Database
- Revoking Issued Certificates
- Creating Certificate Revocation Lists (CRLs)
- Viewing CRLs

Displaying the Certificate Services Log and Database

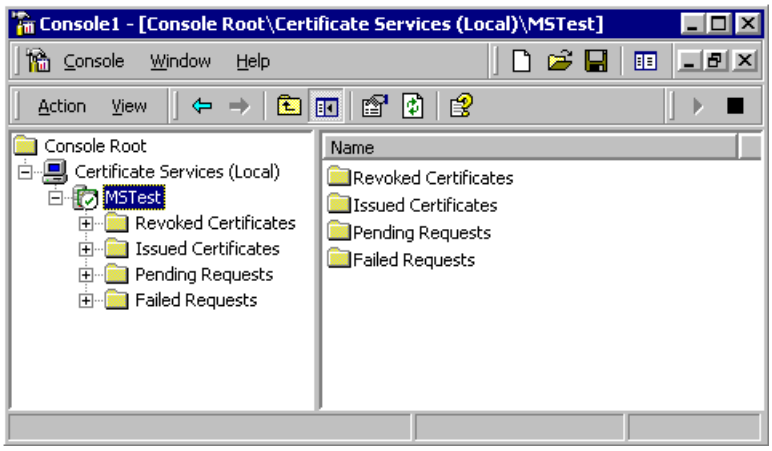
See the section on Known Errors at the end of this document prior to attempting this walkthrough.

Displaying the log and database is useful for performing manual audits of queued requests and issued certificates. It is also useful for identifying and selecting certificates for revocation.

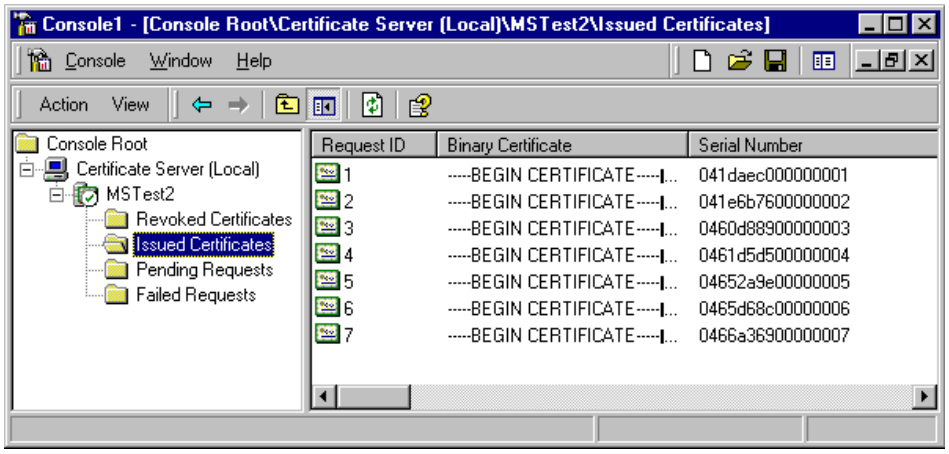
The Certificate Services Log and Database is viewed using the Certificate Services Manager MMC snap-in. This walkthrough uses the snap-in to display the contents of the log and customize the output to see selected data items and records of interest.

To display the log

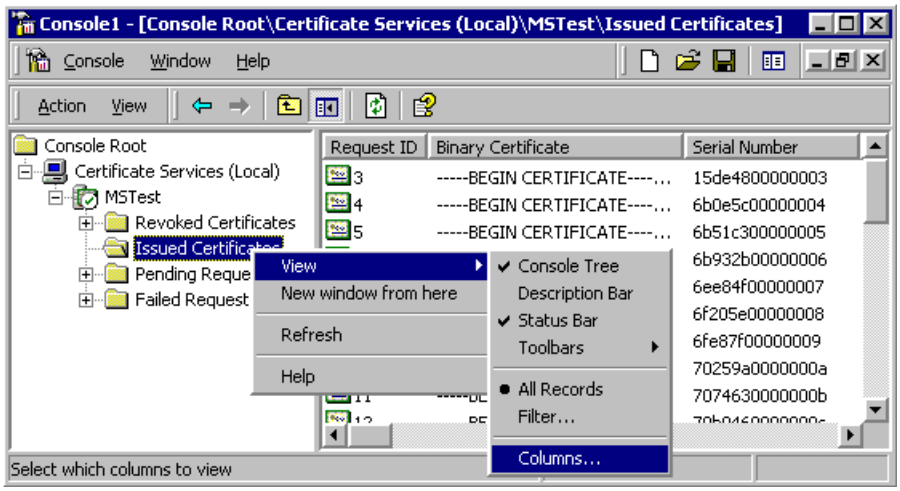
1. Start the Certificate Services Manager snap-in by first starting MMC and then adding the snap-in. Then expand MSTest.



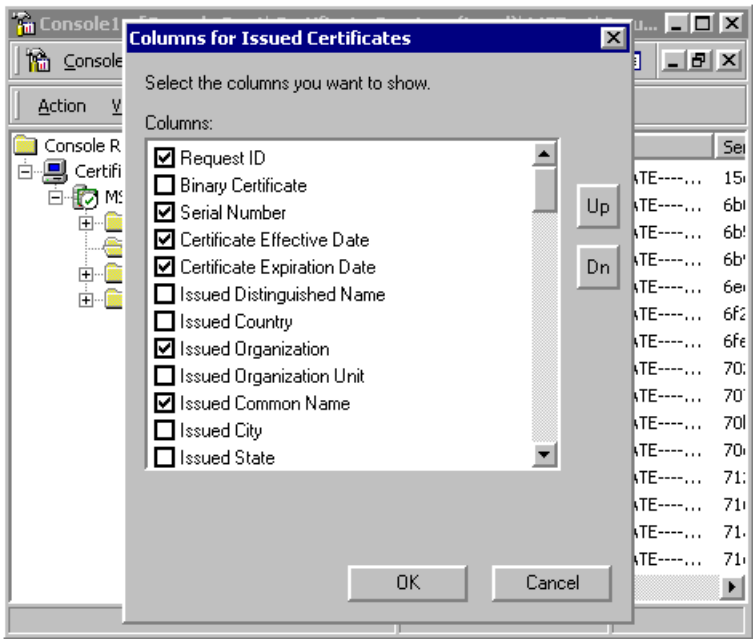
2. To display the log of issued certificates, double-click **Issued Certificates**.



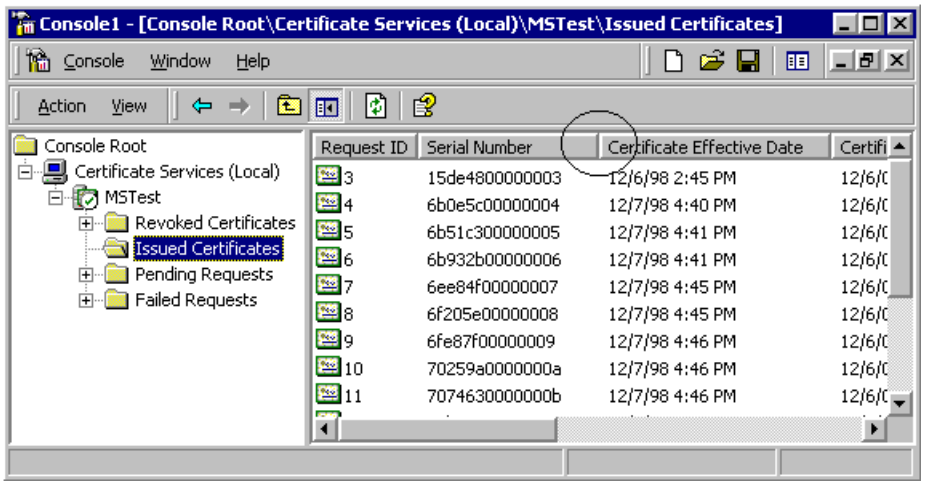
3. Customize the output to display only selected fields. Right click **Issued Certificates**, select **View**, and then select **Columns**.



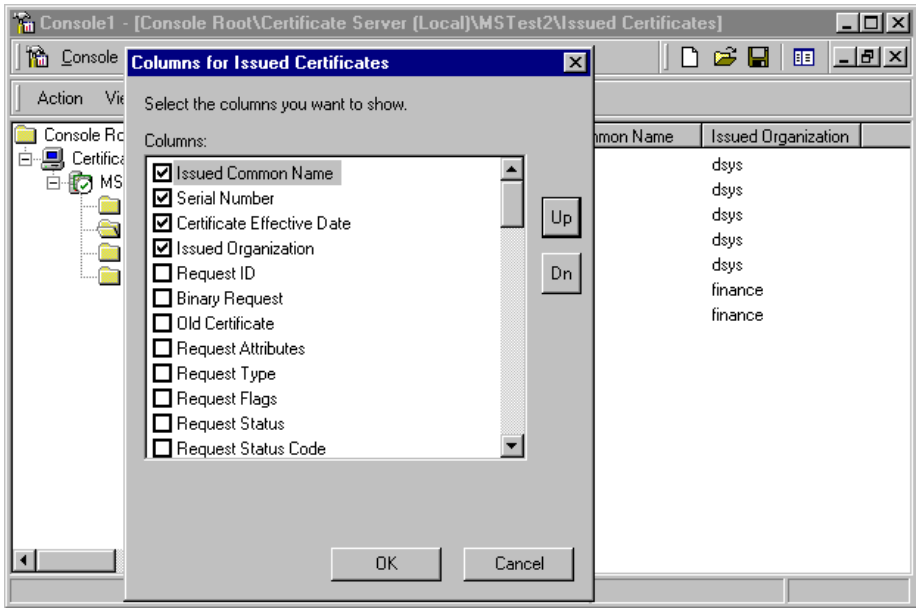
4. Select the fields you want to see. In this example, you should select **Request ID**, **Serial Number**, **Effective Date**, **Expiration Date**, **Organization**, and **Common Name**. Click **OK**.



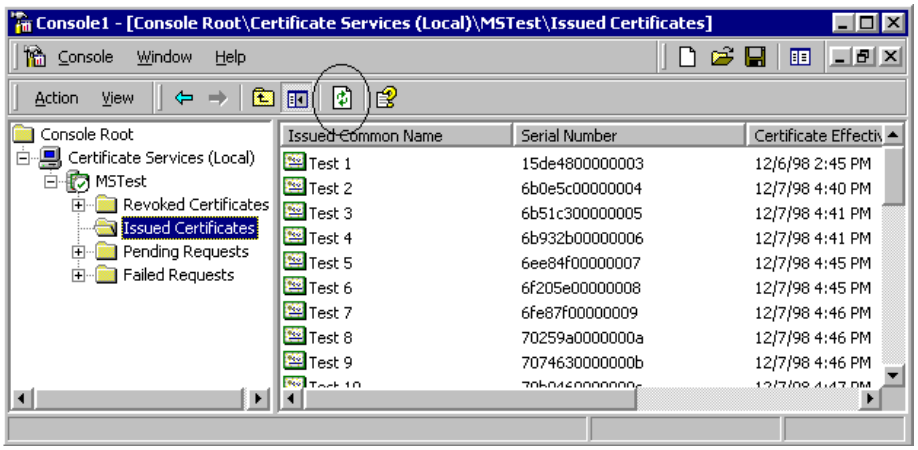
5. Adjust the **column widths** to fit the screen. To do this, position the mouse pointer over the column boundary (shown by the red circle) and adjust left or right as needed.



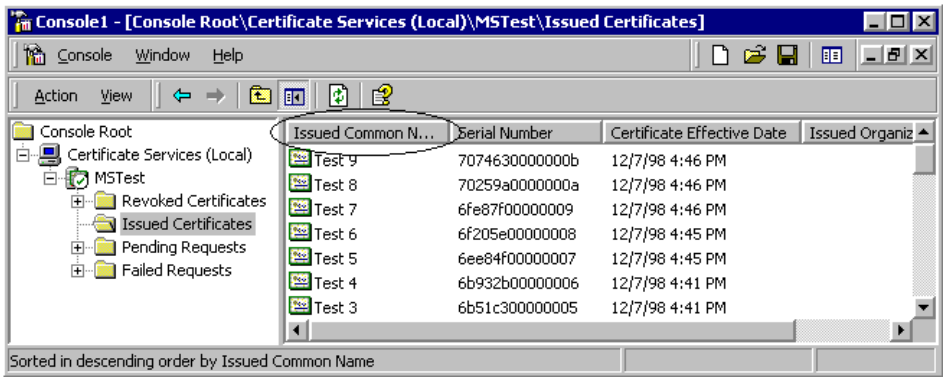
6. To change the order of the columns displayed, right click the **Issued Certificates** folder and navigate to **View**, **Columns** (as done above). Select **Issued Common Name** and click the **Up** button until the **Issued Common Name** field appears at the top of the list.



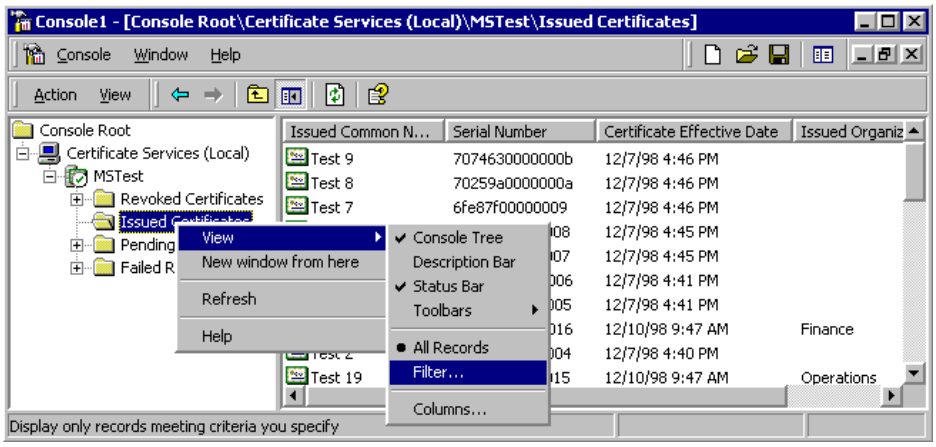
7. **Issued Common Name** is now the leftmost field in the columns of fields in the results pane. Click **OK**, followed by **Refresh** (see the red circle, below).



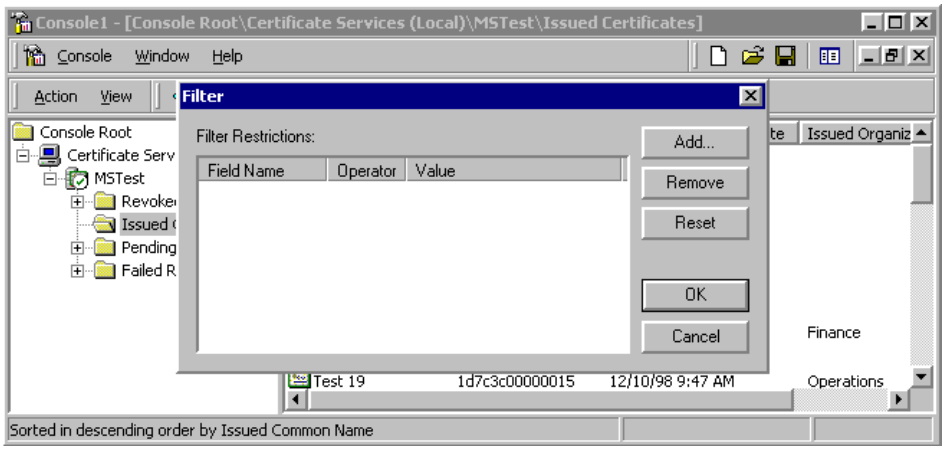
8. Sort the records in reverse order by Issued Common Name, by clicking the **Issued Common Name** column heading.



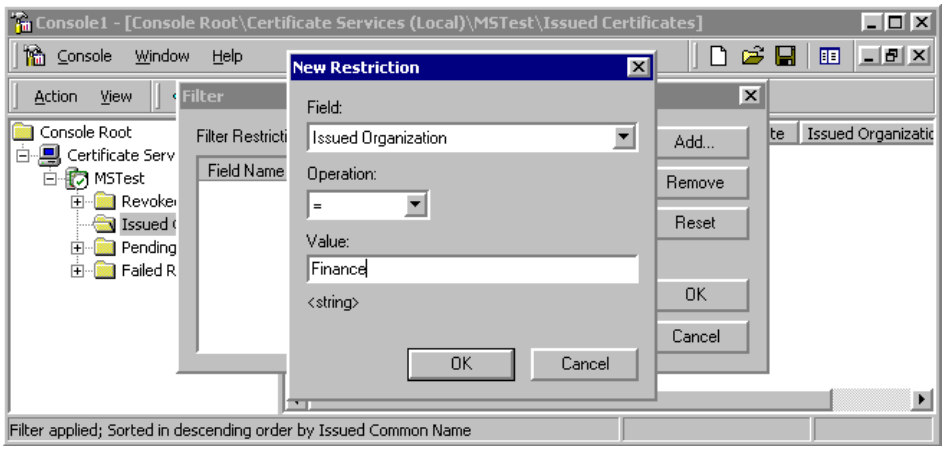
9. Put a filter on the database so that only the **Finance** organization certificates are displayed. Right click **Issued Certificates**. Select **View** and then select **Filter**.



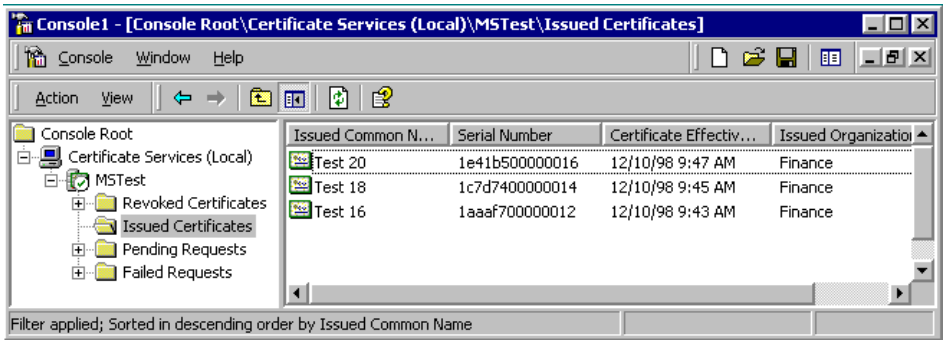
10. Click **Add**.



11. Set the restriction to **Issued Common Name=Finance**



12. Click **OK**, then click **OK**, again.



Revoking Issued Certificates

See the Known Errors section before performing this walkthrough.

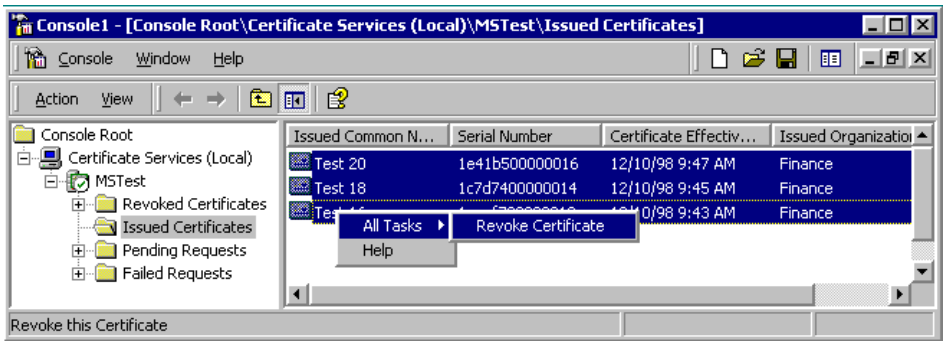
In Certificate Services, to revoke a certificate means to mark an issued certificate in the database as being revoked. Revocation of certificates is useful, because it is a mechanism for invalidating a certificate prior to its natural expiration. Applications that then check the revocation status of a certificate prior to use can then make a more informed decision about certificate validity and what processing to perform.

It is important to note that merely revoking a certificate is not sufficient to make this information available to applications. That requires creation and publication of a Certificate Revocation List (CRL). See the section below on **Creating Certificate Revocation Lists**.

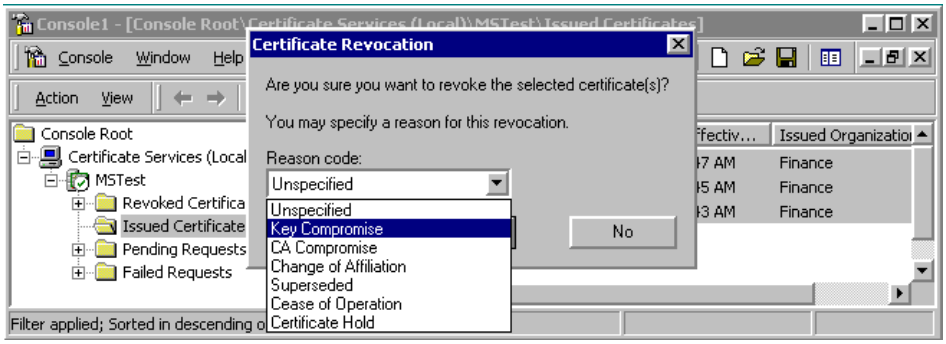
Using the two certificates above, perform a revocation as described next.

To revoke certificates

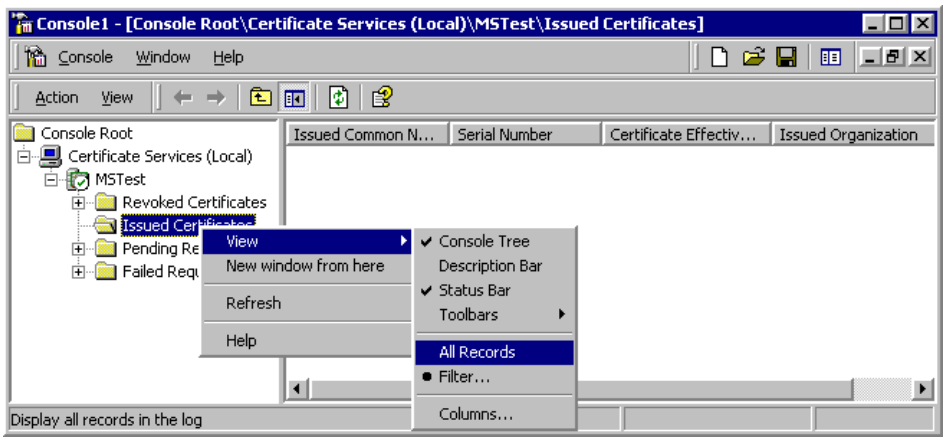
1. Using the filter from the previous exercise, select the Finance group certificates by clicking the first certificate and then pressing shift while clicking the last certificate. Right click the **selected certificates** and select **Task**, then select **Revoke Certificate**.

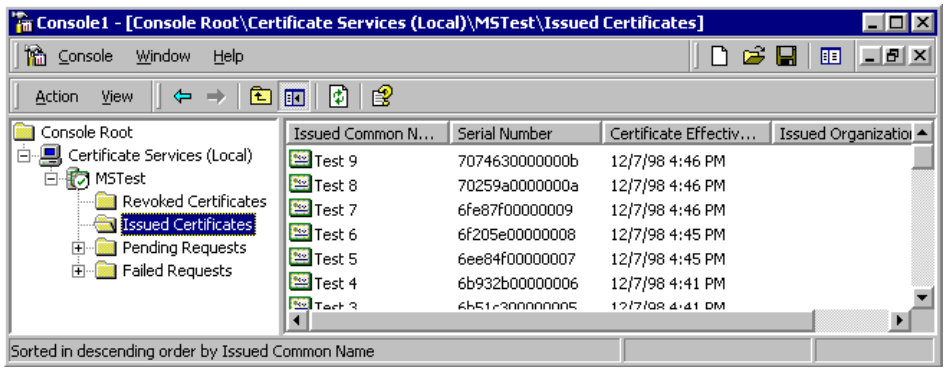


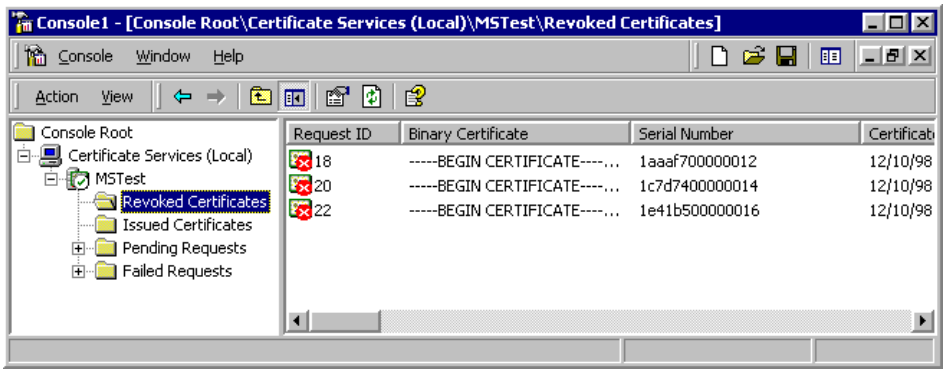
2. Select the reason for the revocation reason using the drop-down list box. For this example, select **Key Compromise**. Click **Yes** after you select the correct reason code.



3. Verify that the revoked certificates are correctly marked in the database. Do this by viewing the contents of the **Issued Certificates folder** and the **Revoked Certificates** folder. The revoked certificates should appear in the latter, but not in the former.





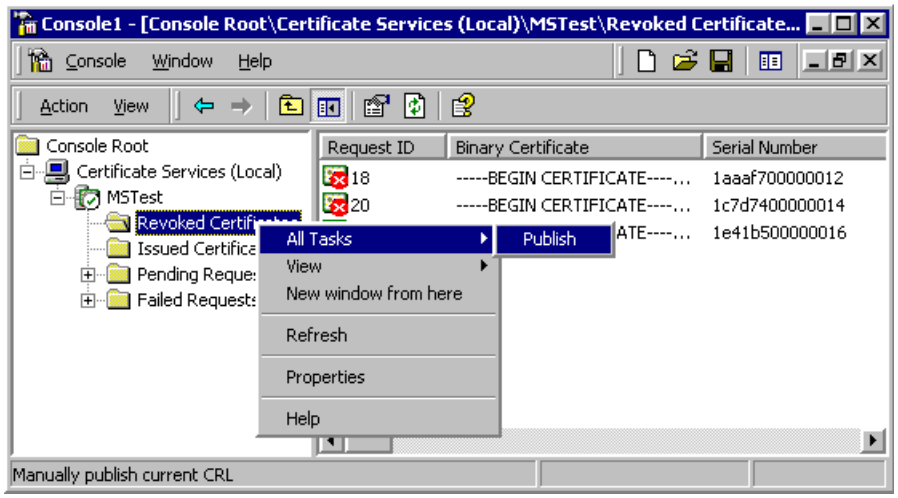


Creating Certificate Revocation Lists (CRLs)

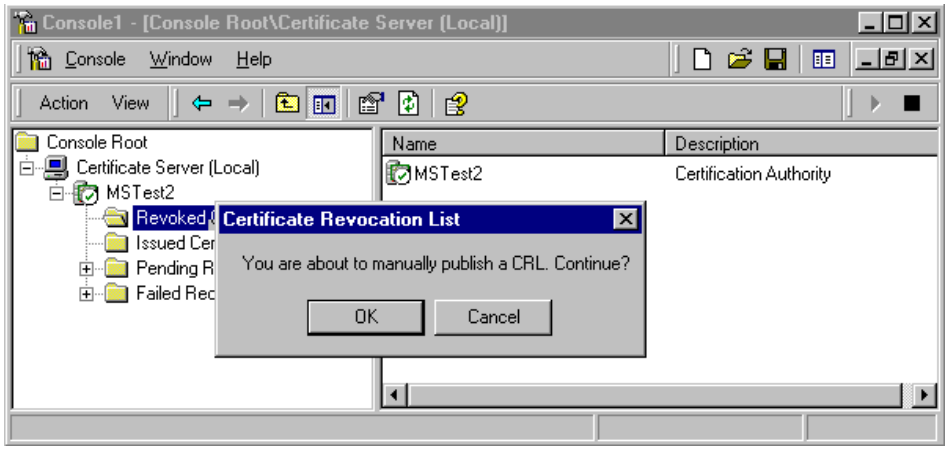
Now that certificates have been revoked, it is necessary to create a Certificate Revocation List (CRL) and publish it so that applications that perform revocation checking have something to check.

To create CRLs

1. Right click the **Revoked Certificates** folder. Select **All Tasks** and then select **Publish**.



2. Select **Publish**.



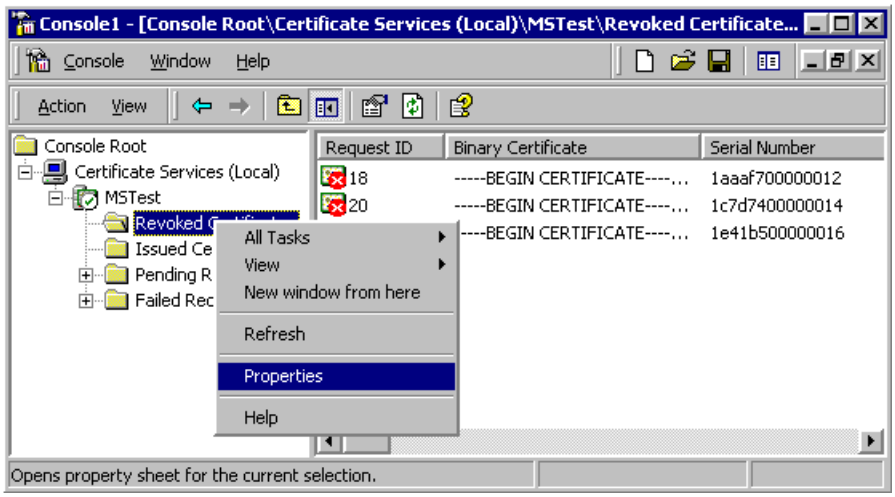
3. Click **OK**.

Viewing CRLs

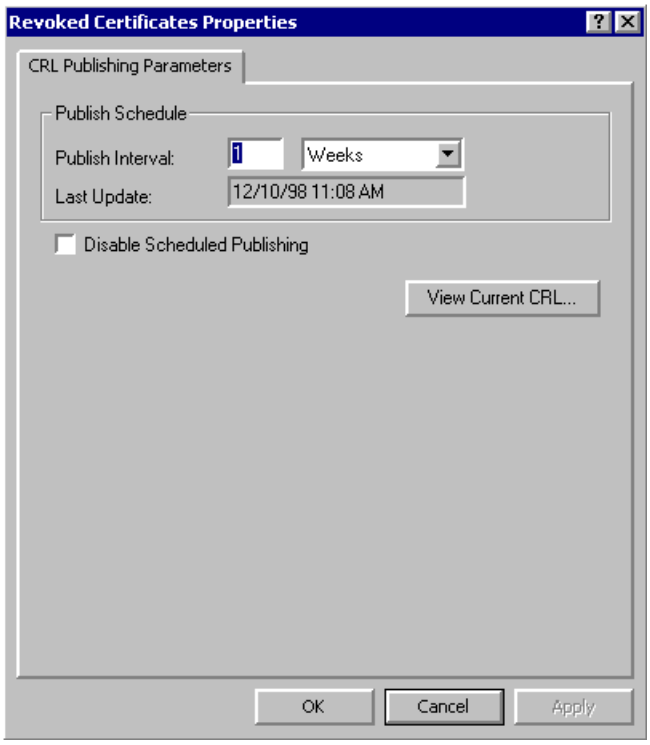
The CRL has now been published. Verify that it is correct.

To view the newly published CRL

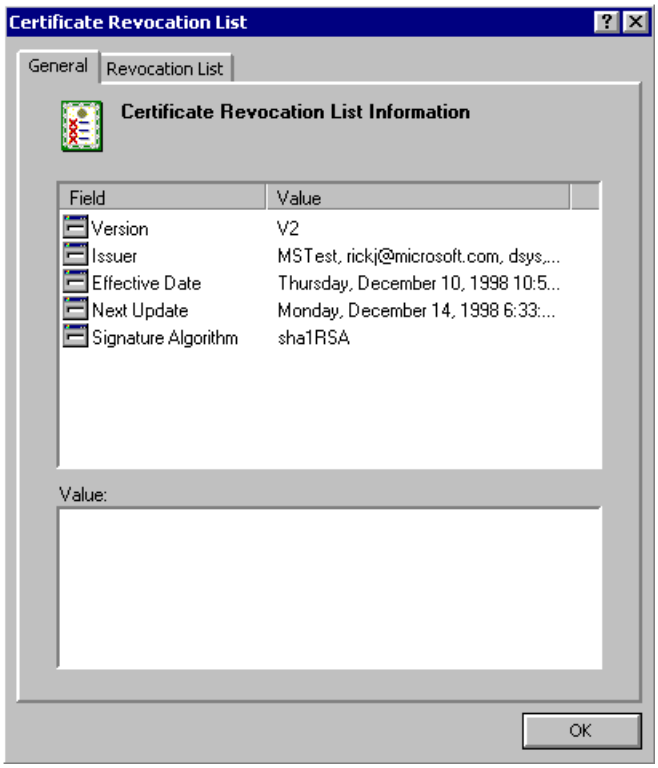
1. Right click the **CA** node, and select **Properties**.



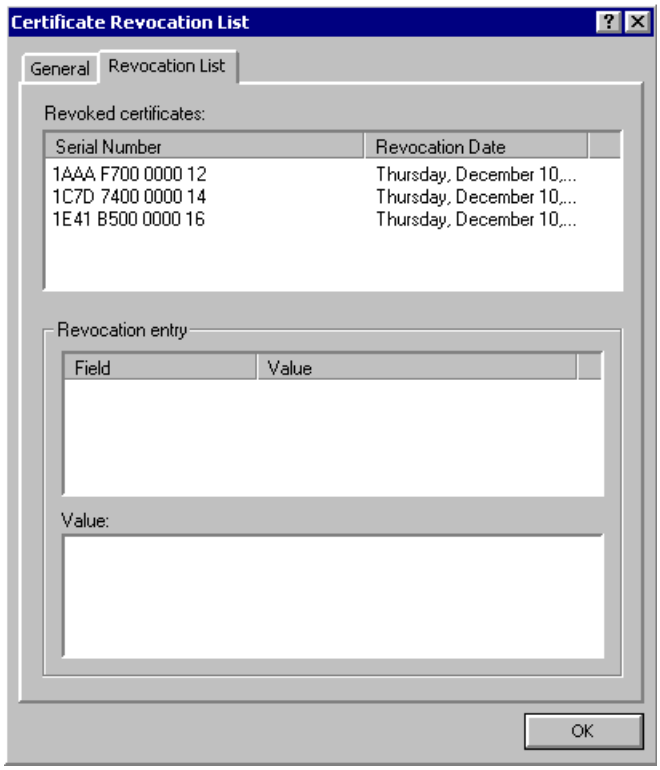
2. Click **View Current CRL**.



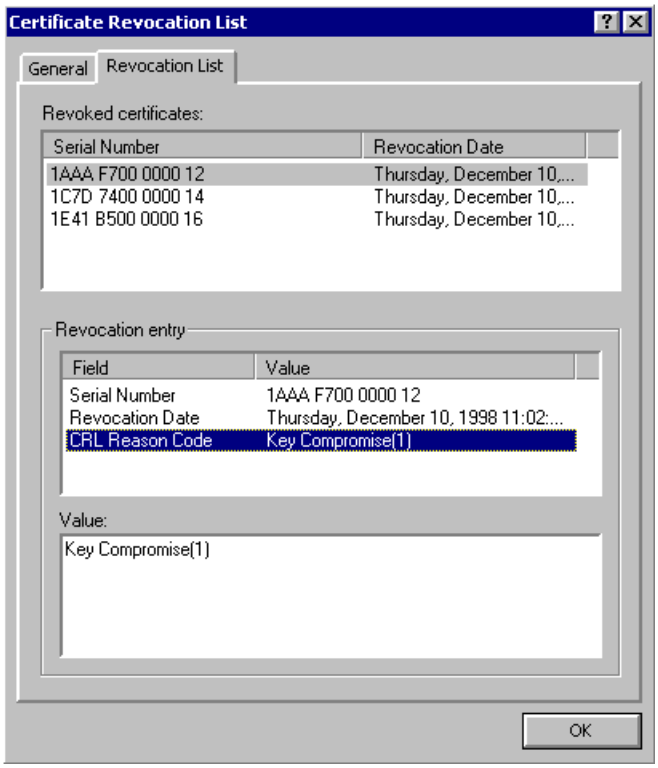
3. This form provides overall identification information for the CRL.



4. To view the CRL contents, click the **Revocation List** tab.



5. To view details on a particular revoked certificate, select it. The details are displayed in the **Revocation Entry** box. The **Value** box is provided in case the field values are too large for the **Field/Value** pair. Selecting one of the **Field** entries displays the full contents of the selected field.



KNOWN ERRORS

- Backup/Restore Limitations: If Certificate Services is installed with the DSS Cryptographic Service Provider, then Certificate Services Backup does not function correctly in Beta 3. This is not a problem if Certificate Services is installed with one of the RSA Cryptographic Service Providers. This will be fixed in a future release.
- Known Problem in Restore CA: The Restore CA function does not look in the correct place for its restore information in RC0 (Build 1946). As a result, the files containing this information must be manually placed where restore can locate them. Perform the following steps prior to performing the restore:
  - Erase the existing contents of %windir%\system32\CertLog.
  - Copy files from the backup database directory to the CertLog directory, e.g., – copy c:\bkup\DataBase*.* %windir%\system32\CertLog.
  - Perform the restore as described.

  This will be fixed in a future release.
- Adding the Certificate Services MMC Snap-in: On the first use of the Certificate Services snap-in after its addition to the MMC, there may appear one or more error messages stating that the snap-in initialization failed. Ignore these by clicking **OK** and continuing with the walkthrough.

FOR MORE INFORMATION

For the latest information on Microsoft Windows 2000 network operating system, visit our World Wide Web site at http://www.microsoft.com/windows/server/ and the Windows NT Server Forum on the Microsoft Network (GOWORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at http://ntbeta.microsoft.com/.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.